virus BULLETIN

EXTRAITS DES COMPARATIFS ISSUS DES TESTS VBSPAM ET VB100 DE VIRUS BULLETIN : MAI, JUIN, JUILLET, SEPTEMBRE ET OCTOBRE 2010

COMPARATIFS VBSPAM

Le test VBSpam envoie deux flux de spam existants vers tous les filtres soumis à l'analyse par ordre aléatoire, ce qui permet de les exposer en temps réel au même flux de messagerie. Il teste également le produit en lui envoyant, aussi en temps réel, des centaines de messages légitimes. Le test mesure à la fois le taux de faux positifs et le taux d'interception du spam des produits visés. En fonction de ces mesures, l'on définit un point de référence. Tous les produits obtenant un résultat supérieur à ce point de référence se voient attribuer une certification VBSpam.

De plus amples informations concernant la méthodologie du test sont données sur le site :
http://www.virusbtn.com/vbspam/methodology/

CERTIFICATION

Une certification VBSpam est attribuée en fonction du 'score final' d'un produit. Pour obtenir celui-ci, l'on multiplie le taux de faux positifs (le pourcentage de messages légitimes bloqués) par trois, puis on soustrait ce chiffre au taux d'interception du spam (le pourcentage de spam bloqué). Le produit obtient la certification si la valeur de (IS - 3x[FP]) est supérieure à 96.

$$IS - (3 \times FP) \geq 96$$

Il est important de préciser que les résultats du test sont susceptibles d'être influencés par deux facteurs : le contenu du message et la façon dont le test a été mis en place. Par conséquent, un taux d'IS de 98% obtenu dans un test VBSpam n'équivaut pas forcément à un taux d'IS de 98% mesuré par un client ou dans un test différent.

Cependant, grâce à un contrôle strict des conditions du test ainsi que du contenu (identique) des messages filtrés, il est possible de comparer plusieurs produits testés au cours du même test VBSpam. Le test VBSpam est donc très fiable pour évaluer la performance d'un produit par rapport à ses concurrents.

Mai 2010 : BitDefender Security for Mail Servers 3.0.2

Taux IS : 99,55%
Taux IS (contenu VB) : 91,15%
Taux IS (spam image) : 99,61%
Taux IS (spam volumineux) : 99,78%
Taux FP : 0,14%
Taux FP (contenu VB) : 0,50%
Score final : 99,14

Les développeurs de BitDefender soumettent leur produit aux tests de Virus Bulletin depuis son tout premier test anti-spam. Déjà récompensé six fois, BitDefender se voit attribuer ce mois-ci sa septième certification VBSpam. Il devient ainsi non seulement le seul produit à avoir été récompensé dans tous les tests VBSpam, mais il réalise cet exploit avec un taux d'interception de spam très respectable et juste trois faux positifs, et obtient le deuxième meilleur score final du test de mai 2010.

Juillet 2010 : BitDefender Security for Mail Servers 3.0.2

Taux IS : 99,91%
Taux IS (spam image) : 99,89%
Taux IS (spam volumineux) : 99.69%
Taux FP : 0.00%
Score final : 99,91

Au cours du test de mai 2010, *BitDefender* a obtenu un excellent taux d'interception de spam et seulement trois faux positifs : trois de trop selon ses développeurs. Ceux-ci ont donc été enchantés d'apprendre qu'aucun faux positif n'avait été détecté au cours du test de juillet et que le taux d'interception de spam était demeuré identique au précédent.

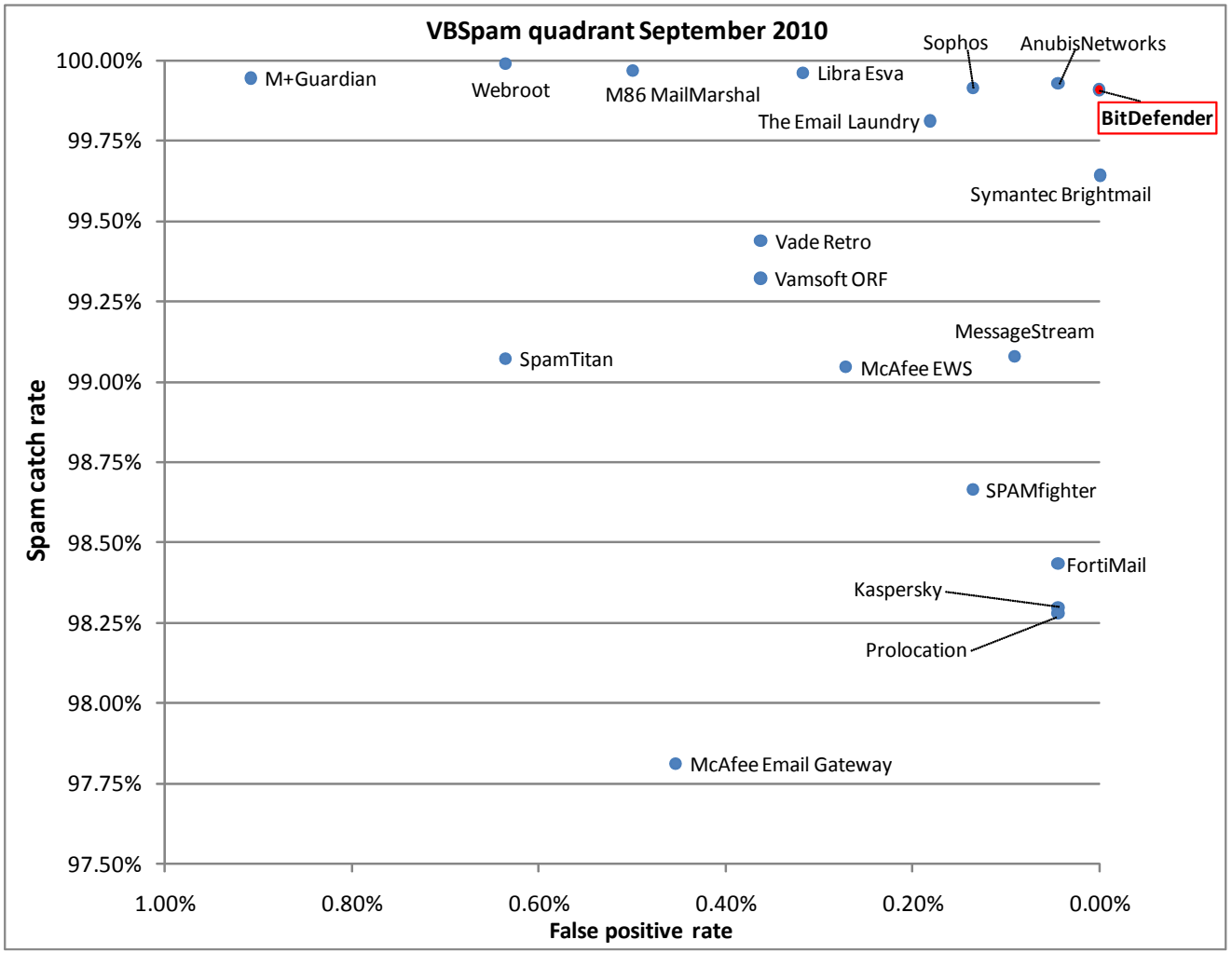
Obtenant une fois de plus l'un des scores finaux les plus élevés, le produit Roumain gagne sa huitième certification VBSpam consécutive.

Septembre 2010 : BitDefender Security for Mail Servers 3.0.2

Taux IS : 99,91%
Taux IS (spam image) : 99.81%
Taux IS (spam volumineux) : 99.20%
Taux IS pré-DATA : NA
Taux FP : 0.00%
Score final : 99,91

C'est toujours bon signe de rencontrer des développeurs confiants en la qualité de leur produit : ceux de *BitDefender* n'ont pas hésité une seconde à soumettre leur produit aux premiers tests VBSpam. Leur assurance ne les empêche pas de travailler sans relâche à l'amélioration de leur produit et ils sont toujours ouverts à recevoir des commentaires concernant sa performance.

BitDefender Security for Mail Servers est le seul produit à s'être vu attribuer une récompense dans tous les tests VBSpam sans exception.
De plus, avec l'un des taux d'interception de spam les plus élevés du test et aucun faux positif, le produit a battu tous ses compétiteurs en se classant en tête du test de septembre 2010.



VIRUS BULLETIN VB100 ANALYSE ANTI-MALWARE

Pour qu'un produit anti-malware obtienne une certification VB100 il doit détecter par défaut (à la demande et à l'accès) tous les malwares reconnus en circulation au moment de l'analyse, et ne doit générer aucun faux positif lors du contrôle de fichiers sains.

Les produits sont soumis à d'autres tests au cours du processus comparatif : l'on mesure notamment la vitesse et l'impact sur les performances du système et l'on effectue des tests RAP (Reactive and Proactive).

Les tests RAP mesurent l'aptitude du produit à détecter quatre ensembles distincts d'échantillons de malwares. Les trois premiers sont constitués de malwares rencontrés au cours des trois semaines précédant la soumission du produit aux tests. Ils mesurent la vitesse à laquelle les développeurs et labos réagissent au flux régulier de nouveaux malwares. Le quatrième est constitué d'échantillons de malwares rencontrés la semaine suivant la soumission aux tests. Ce test vise à évaluer, à l'aide de techniques génériques et heuristiques, la capacité de détection proactive d'échantillons de malwares nouveaux et inconnus.

Bien que la certification VB100 d'un produit n'est pas affectée par les résultats de ces tests secondaires, ils donnent au lecteur une meilleure vision globale des performances du produit.

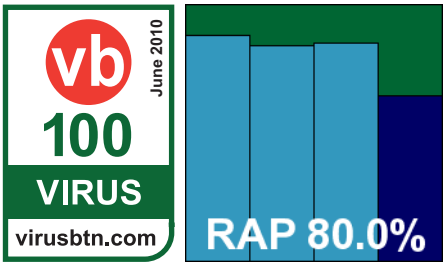
De plus amples informations concernant la méthodologie du processus de certification VB100 sont données sur le site :

http://www.virusbtn.com/vb100/about/100procedure.xml.

Juin 2010 - Windows Server 2008 R2 - BitDefender Security for File Servers 3.4.11.141

ItW	100%	Polymorphe	100%
ItW (o/a)	100%	Chevaux de Troie	93,17%
Vers & bots	92,87%	Faux positifs	0

Solution complète pour serveur, ce produit de BitDefender que l'on contrôle grâce à l'interface MMC est aussi facile à installer qu'à utiliser. De plus, son interface graphique est plus colorée et dynamique que ce que l'on attendrait habituellement de ce genre de logiciel. La navigation dans le produit est intuitive et nos testeurs ont tout particulièrement apprécié le système de planification, qui permet une mise en place simplifiée des tâches telles que l'installation d'un planificateur pour une efficacité optimale. Des problèmes inattendus ont parfois été relevés, c'est le cas notamment de certains sous-dossiers, apparaissant dans les sections sélectionnées, qui ont échappé aux premiers contrôles. Mais après avoir effectué des vérifications minutieuses et réexécuté le test plusieurs fois, nous avons obtenu tous les résultats nécessaires.

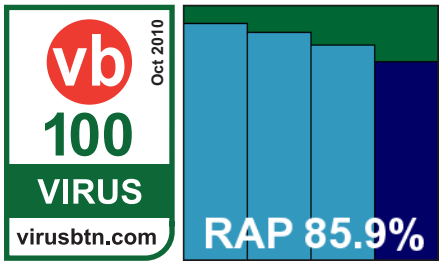


L'on peut rapporter une vitesse de contrôle honorable sur demande et satisfaisante à l'accès une fois le produit familiarisé avec les fichiers. Grâce au graphique d'utilisation des ressources, l'on a pu constater que le produit avait un impact relativement faible sur la mémoire et le processeur. Des taux de détection très respectables ont été obtenus dans les tests principaux ainsi que dans les tests RAP. Le produit a traité la WildList sans efforts, et en l'absence de fausses alarmes, *BitDefender* a rajouté encore une certification VB100 a son palmarès déjà bien rempli.

Octobre 2010 - Windows Server 2003 - BitDefender Security for File Servers 3.4.141

ItW	100%	Polymorphe	100%
ItW (o/a)	100%	Chevaux de Troie	95,42%
Vers & bots	98,88%	Faux positifs	0

Cette solution pour serveur *BitDefender* est un produit professionnel complet à installation rapide malgré l'incorporation de la console MMC, qui n'exige ni redémarrage ni interaction intensive avec l'utilisateur. L'interface est agréable et fait bon usage de la console MMC pour offrir un accès complet et rationnel aux commandes de configuration et de contrôle. Bien qu'honorable lors de la première exécution du test, la vitesse de contrôle est devenue remarquable lors des contrôles suivants des fichiers connus, grâce à l'utilisation de techniques d'interception intelligente. L'on a constaté une faible utilisation du processeur, certainement grâce à ces mêmes techniques. L'encombrement de la mémoire en revanche était un peu en dessus de la moyenne.



Dans les tests comprenant des fichiers infectés, les contrôles s'effectuaient bien jusqu'à la fin mais ne présentaient qu'un écran vide. De meilleurs résultats ont été obtenus en réexécutant les contrôles par plus petits groupes. Ceci suggère que le système de journalisation se laisse facilement dépasser par de grands nombres de détections, mais il faut bien avouer que l'on ne rencontrerait pas ce genre de cas dans le monde réel.

C'est au terme de recherches approfondies que nous avons conclu que nous abandonnions le système de journalisation un peu hâtivement, en général au bout d'une heure environ. Certains rapports apparaissaient après une plus longue période sans réponse.

Au final, nous avons recueilli toutes les informations nécessaires, avec d'excellents scores vis-à-vis des ensembles de fichiers infectés et aucun problème vis-à-vis des fichiers sains. *BitDefender* a donc mérité sa certification VB100.

BitDefender
650 Castro St, Suite 240,
Mountain View, CA 94041, USA
Téléphone : + 1 800 388 8062
Web: www.bitdefender.com